2015-08-23

Managing Digital Risk

Phippen, AD

Bookboon

Simon Ashby & Andy Phippen

Managing digital risk

Managing digital risk
1st edition

ISBN 978-87-403-XXXX-X

Contents

About the Authors

Dr Simon Ashby

Dr Simon Ashby is an Associate Professor of Financial Services at the Plymouth Business School (www.plymouth.ac.uk/business). Prior to this he worked as a financial regulator for the UK Financial Services Authority (writing policy on risk management) and a senior risk manager in a number of top UK financial institutions.

Simon has a PhD in corporate risk management and has published many academic papers and industry reports on risk management in organisations. Along with digital risk management his current research interests include risk appetite, risk culture and operational risk management.

Simon remains actively involved in a number of industry sectors (including financial services and social housing) and is a regular speaker at industry conferences and seminars. He also provides occasional training and consultancy services. Simon is a Fellow of the Institute of Operational Risk (www.ior-institute.org) and is also a Director and Audit and Risk Committee Chair of Plymouth Community Homes (www.plymouthcommunityhomes.co.uk).

Andy Phippen

Andy Phippen is a professor of social responsibility in information technology at the Plymouth Business School, Plymouth University. He has worked with the IT sector for over 15 years in a consultative capacity on issues of digital risk, with companies such as British Telecom, Google and Facebook. He has presented written and oral evidence to parliamentary enquiries related to the public use of ICT and is widely published in the area. In recent years he has specialised in the use of ICTs by young people, carrying out a large amount of grass roots research on issues such as their attitudes toward privacy and data protection, file sharing and internet safety.

1 What is 'Digital Risk'

In this book we explore the concept of "Digital Risk" and the implications of this for organisations. We will explore the traditional focus of the area, and argue that a broader definition, and understanding, of the term is needed as a result of the advent of "digital natives" in the workplace and the evolving nature of the relationship between technology and society. While this may seem like a strange thing to explore within an organisational context, we will argue that, with the blurring of social and professional lives, as a result in part of greater reliance on Information and Communication Technologies (ICTs) in order to perform work functions, we need to be mindful of a whole new range of risk issues outside of the "traditional" boundaries of Information Assurance, the traditional domain of digital risk. In the first half of this book we explore how reliance on similar ICTs for both work and social life and, as a result of the change in social interaction facilitated through technology, introduces a whole new range of risk management issues for both individuals and the organisations for which they work.

The book is structured to explore these potential risk management issues and proposes that social technology has evolved beyond the boundaries of traditional "digital risk management" practices. The book will also argue that when these behaviours are placed in an organisational context, "conventional wisdom" around acceptability and unacceptability cannot be relied upon to protect an organisation from the potential fall-out from a digital incident. By exploring legal precedents, emerging trends and evolving behaviours, we will define a broader context of digital risk before exploring what damage can result from unmanaged risk in this area, the types of harm that result (for example, financial, reputational, business continuity, etc.) and what organisations need do to protect both their employees and themselves from these risks. The second part of the book develops risk management concepts to incorporate these new threats, and will conclude by proposing a new model of digital risk management which encompasses the broader digital risk context, as well as highlighting the importance of "horizon scanning" in this area and being proactive in response, thereby establishing effective protection through due diligence, rather than only dealing with issues when they emerge.

We will begin with an exploration of the contested concept of the Digital Native, and their influence in the workplace. This is an important starting point because, while contentious in its completeness and empirical manifestation, it does allow us to explore the change in society that has resulted from the mass adoption of ICTs, particularly social technologies, and how this transfers into the workplace context.

The concept of the "Digital Native" defines individuals who have only known a world with the presence of the Internet. The term was first proposed by Prensky (2001a,b), when he stated that the physiological structure of the brain and cognition patterns of Digital Natives fundamentally differs to that of other generations. They were born post-1990 and typically the younger siblings of Generation X (Whittaker, 2010a,b) or children of the older Baby Boomers and Veterans (Penna, 2008). The term and classification of this identified population is relatively recent and open for debate, indeed, the term "Millennial" has gained greater acceptance and Howe and Strauss (2007) define generations as follows:

Generation	Birth Year	Pseudonyms
Veterans	1925–1942	Traditionalists, WWII generation, the Silent Generation
Boomers	1943–1980	Young Crusaders
Generation X	1961–1981	Baby Busters, Nomads
Millennial	1982–	Gen Y, Generation Net, Internet Generation

Table 1.1 – Generational definitions as proposed by Howe and Strauss (2007)

In their work, Howe and Strauss discuss how each generation demonstrates certain characteristics and observable patterns. However, they also stress that these are easier to see in hindsight. We can argue that the emerging generation will demonstrate different attitudes and behaviours at work than those before, however, with the Millennial generation it is difficult to have a complete impression of what these differences are.

Regardless of terminology, it is clear that we are now recognising a young workforce who have never experienced a time without Internet access and digital technology. Their expectations and perceptions of any manner of stimuli differ, from the way they perceive/conceptualise time to fundamental business etiquette (Lewis, 2010). Parry (2009, p. 6) supports this position, stating "younger generations, particularly employees who entered the workforce after 1990 are more likely than older generations to be familiar with and comfortable with using emerging information and communication technology."

In their critique of the 'Digital Native' debate Bennett, Matton and Kervin (2008) conclude that research on young people's relationships with technology is much more complex than the Digital Native characterisation suggests, and that young peoples' technology use and skills are not uniform. In addition, the literature could not show evidence of widespread and universal disaffection or distinctly different learning styles. This is noteworthy in so far as it disputes that the generation emerging from the digital age is reminiscent of a black swan event (Taleb, 2008) or "singularity" as purported by, for example, Prensky (2001a,b), Tapscott (1998) and Howe and Strauss (2000). In short it may be that while Digital Natives are different, they are not a completely new breed.

As acknowledged above, while there is much active debate surrounding how Digital Natives and their "Immigrant" older peers are defined in conjunction with scrutiny of the lacking empirical evidence to support this concept, Bennett, Matton and Kervin, (2008) going so far as to accuse academics of causing moral panic. Taxonomies have been developed on nuances of Prensky's (2001a,b) initial and controversial publications and alternative theories have been proposed, most notably the Visitor-Resident model (White, 2011) and the relationship between the Digital Renegade and Digital Captive (Morozov, 2008).

However, what is clear is that many scholars do acknowledge that digital technology, particularly in the social world (i.e. social media), does have the *potential* to influence behavioural norms in both society and the workplace. Therefore, it is important for organisations to be aware that the next generation of employees *may* exhibit behaviours that differ from their existing workforce, as a result of technological engagement and the issues that may arise from those who do not differentiate between the online and offline world. It is also important to note that while the younger generation tend to be early adopters of technology (Livingstone and Helsper 2007), the behaviours, and associated technologies, will also become adopted by older generations as they become mainstream. This is explored in more detail in chapters two and three but it should be stressed from the outset that what we are proposing in this text is not simply extending risk management to deal with "younger" employees, but to acknowledge that the "Internet Generation" has lead a changes in behaviour adopted by society as a whole.

A simple example of this, which allows us to consider all manner of issues around technological normalisation and acceptability, is the recent case of 4 high court judges being dismissed for accessing pornography during work time[1] "inexcusable misuse" of their official accounts and "wholly unacceptable conduct for a judicial office holder" were given as the official reason for their dismissal (three judges were sacked, one resigned). Taken at face value, this might be considered very straightforward – who would disagree that members of the judiciary should not access pornography at work? However, it does raise some interesting issues that demonstrate both the evolving nature of digital risk and also how organisations address this.

For example, let us first explore the act itself – accessing pornography at work. It has been stressed in all reporting of the case that the content accessed was not illegal of itself. While, if we apply common sense to the issue, we might say that accessing pornography at work is wrong, can common sense be applied in a risk management context? Has the organisation made it clear to their employees that accessing "inappropriate" content in work time is unacceptable, and if so, why is this the case? In another case in Canada, a civil servant called Franklin Andrews[2] as dismissed for accessing pornography at work due to "time theft" and later reinstated when it could not be demonstrated his job was not being performed fully as a result of this "inappropriate" access.

Secondly, we have to ask how did the organisation become aware that their employees are accessing pornography? We would anticipate that this was done through either analysis of Internet access logs or discrete access monitoring software. The employer in this case has declined to comment on how the access was discovered, but it is clear that this discovery was as a result of some form of monitoring, either live or retrospective. If this is the case, were staff aware that this was the case? If so, why were they accessing pornography at work? Perhaps it was naivety on the part of the employees, or perhaps they were not aware monitoring was happening. The issue of monitoring access is a contentious one and something we will return to later, as there have been arguments that covert monitoring is an invasion of an employee's human rights.

We should also consider a comparison of the offline and online in this case. Would an employee face similar dismissal for looking at a pornographic magazine at work? And how would an employer know that the employee had been looking at a pornographic magazine? Clearly there are some fundamental differences between the online and offline versions of access to pornography – for one it would be unlikely that an employer had provided the facilities to access pornography if the content took the form of a magazine, whereas with online access, one might argue that facilitation has certainly occurred through infrastructure provided by the organisation. Therefore, the organisation are more likely to try protect themselves, and take a harsher view, of accessing pornography online, especially given they are more likely to discover it than if access was offline. And if this is the case, the employer certainly runs the risk of reputational damage if they are not seen to act upon such a matter – would the press be friendly if they were to discover (for example, through Freedom of Information requests) that employees in the judiciary were accessing pornography at work and this was known by the employer?

However, this does lead to the final point, which is far more philosophical in nature – if the reason for dismissal was "inexcusable misuse" of their official accounts and "wholly unacceptable conduct for a judicial office holder" who has made those, essentially, moral decisions, given that it was already stated that the access to content was not, of itself, illegal? Again, while we might suggest that common sense should take part in this decision, if the employee felt that they were still performing the job to the best of their abilities, what was "wholly unacceptable" about their conduct? The use of ICTs to access material not related to their job role at work? Or access to pornography? If it is the former, then has the employer made it clear the level of access to non-work related content that is acceptable at work (not at all, only in lunchtimes, only certain types of content, etc.)? Would "inexcusable misuse" extend to, for example, an employee accessing Facebook in work time? And if it is the latter, what is so different about access to legal pornography, compared to other, potentially socially unacceptable, forms of content such as disagreeable political content or gambling? And finally, if we are to accept that an organisation can be an arbiter of acceptable content within a work context (and why should they not be?) why would they not put technological countermeasures in place to try to ensure that such content cannot be accessed. While the fallibility of filtering solutions is well documented (for example, Techdirt 2014)) such a practice would at least send a clear message of unacceptability to employees which could be reinforced through policy and training.

Even within this, on the face of it, clear and straightforward case, we see that digital risk needs to consider a wide range of issues that move outside of the traditional domain of protecting assets and information. We have, in this single case, issues of social acceptability verses what the employer might view as unacceptable, how discovery was made, whether employees had been made aware of their employer's moral judgements and, if so, whether this was clearly articulated to the employee. Moreover, while we might observe that these sorts of behaviours are the domain of the "digital natives" this case clearly demonstrates that they are not limited to younger members of the workforce. However, what is clear is it is the advent of Internet enabled technologies in the workplace that allow such practices to happen. The idea that, in a pre-Internet (or, more correctly, World Wide Web) era, an employee could use ICTs provided by their employer to access sexually explicit material would be unthinkable and, although potentially possible, virtually unheard of.

In the next chapter we explore this concept in more detail as we define the traditional boundaries of information assurance, the traditional domain for digital risk, before expanding them by exploring the potential areas of risk that can emerge if we are to also incorporate social technologies and normalised digital behaviours into the mix. This is extended further into the third chapter where we look at the potential moral issues that might arise when applying these issues in the risk management framework, before considering both legal and "ethical" dilemmas that an organisation may face as a result, before looking, in subsequent chapters, on how they might build greater resilience into a digital risk management framework.

2 Extending Digital Risk

Digital risk traditionally falls within the field of Information Assurance (IA), the practice of assuring that organisations' information and technical resources are secure, accessible only by those who are allowed to, are used only for the purposes they are intended and are complete and intact. The following chapter explores this in more detail before we return to these issues within a risk management context, but an argument we will return to repeatedly in this book is that traditional, predominantly technologically focussed, countermeasures soon break down if we are to consider social behaviours brought into the workplace via technology. Within this chapter we do not intend to conduct a comprehensive audit of the whole Information Assurance domain, but to present key facets in order to build the case for the need to extend outside of the IA domain when considering emergent practices.

Information Assurance and its strong alignment with IT Systems Security is a well-established discipline that marries risk management with the IT systems, practices and policies of an organisation, applying aspects of corporate governance to the technical infrastructure of an organisation (see Cummings, 2002; Kankanhalli et al, 2003). Ultimately, it is in place to protect the *information assets* of an organisation and the related standards (CoBIT, Risk IT, ISO/IEC 27002)) are used by "hundreds of thousands" of organisations (Humphreys 2008, p. 247). Generally Information Assurance is broken down into a number of distinct areas

- Integrity – Information assets are accurate and complete within an organisation
- Availability – Information assets are available when needed
- Authenticity – Information assets are genuine and their sources are valid
- Non-reputation – transactions and communications of information assets are valid and cannot be denied
- Confidentiality – only those who have the right to access information assets are able to

In order to address these issues the standards will usually define a number of different procedures and practices that will decompose into a number of different areas such as:

- Technical controls – system based safeguards such as access control, malware protection, etc.
- Physical controls – physical prevention of access (secure rooms, locked doors, etc.), protection from theft, fire prevention
- Procedural controls – policies, effective risk assessments and auditing, business continuity planning, asset management
- People controls – effective recruitment practices, proper staff training and awareness programmes, etc.
- Legal control – the need to comply with relevant legislation, the need for awareness of legal issues that might result from a breach

Therefore, as we can see from the definitions above, the actions of people within organisations are already defined within the Information Assurance domain. According to the BIS IT Security Breaches 2014 survey (BIS, 2014) almost 50% of respondents in a survey of over 1000 UK organisations had experienced "staff related issues" in the last 12 months. The definitions of "staff related issues" were quite narrow in focus, relating to:

- Unauthorised access to systems or data
- Breach of data protection law or regulation
- Misuse of confidential information
- Loss or leak of confidential information

From an Information Assurance point of view the emergence of "Digital Natives" or, the evolution of social digital practice, into the workplace greatly extends what we need to think about around "people controls" or "people risk". We would argue that Emergent Digital Risk goes far beyond these traditional boundaries, where the focus is that individuals employed by an organisation are correctly recruited and trained to be able to use the ICTs required to conduct their jobs, while retaining assurance of information assets within the organisation. What it fails to do is consider prior knowledge or behaviours and how this might manifest in the workplace. This should not be surprising, it has only been in recent history that such things would be an issue, even twenty years ago an organisation would not expect new employees to come in with many years experience using ICTs within a social setting and potentially having developed their skills and awareness via informal peer learning rather than traditional education or workplace training.

Therefore, while this concept of "people risk" within the Information Assurance domain does seem narrow, if we are going to expand the concept of digital risk beyond information assurance to incorporate social digital behaviour, we would certainly not dismiss the importance of maintaining effective information assurance as an element within effective risk management. Indeed, with the emerging Millennial workforce, we would argue that this is more important than ever and would further argue that social digital behaviours would increase the risks associated within the Information Assurance domain, particularly around those sorts of issues identified in the BIS 2014 survey. However, we also need to consider how prior knowledge or poor behaviours results in what we might refer to as "traditional" Information Assurance risks. If we are to take the issue of data protection breaches – where information assets might be used in a manner not defined in the data usage policies of the organisation (or how they have been declared to the data protection regulator) a lack of awareness of such issues may result in an accidental breach. For example, an individual might copy information onto another device, take it outside of the workplace environment or send to others using unsecured communications, without ever thinking about the data protection implications. If an individual is very familiar with the use of ICTs in the social lives, but has not received any education or training around the workplace implications of data use, retention or distribution we can see how easy it might be for them to accidentally cause a breach.

Similarly if we are to consider unauthorised access, this does not specifically have to come from someone gaining access via a password or fraudulently obtained login. Take, for example, the practice of "Fraping" (for a dictionary definition, see: http://www.collinsdictionary.com/dictionary/english/frape) and similar activities on social media sites, where an individual makes modification to another's status or posts while impersonating them; something, in our experience, that is very popular with young people. Though we would view this as unauthorised access, we have an emergent workforce starting employment which often views this sort of practice as humorous and harmless. As a result there is greater potential for unauthorised access to be carried out by such young people without thought of the potential breaches in policy or law.

By way of further example, the recent breach of iCloud, which resulted in the leaking of photographs, some highly personal, of a number of celebrities[3] ultimately was as a result of poor password security and a lack of awareness of phishing and brute force cracking – once again poor social use of technology can be demonstrated to have a potentially highly risky impact within a workplace setting.

There have been concerns about the quality of digital awareness for a number of years. Furnell and Phippen (2007) conducted both qualitative work with young people and also a detailed document analysis of UK schools ICT and Personal, Social and Health Education (PSHE) curricula and identified a number of concerning issues:

- young people having a lax attitude toward fundamental IT security principles such as password protection, unauthorised access and privacy;
- uncertainty regarding how to report incidents relate to security breaches or risky social behaviour facilitated by technology;
- curricula lacking in structured education around privacy, security awareness, online safety and social uses of technology.

And while, in some cases (for example UK new computing curriculum (UK Government 2015) and Common Sense Media Curriculum[4] in the US) there is now more explicit reference to learning about digital technologies in and certainly greater resources, there is still scant evidence to show a consistent level of education being delivered to all young people. For example, in Phippen (2014) a study of over 5000 schools in the UK demonstrated that IT literacy and education around the safe use of technologies was in general not well delivered and issues such as staff training, which is fundamental in ensuring a consistent approach to education within the establishment, was generally one of the weakest aspects in schools.

Therefore, we have serious cause for concern – if this emerging workforce is lacking in awareness of even the basic requirements of how to use ICTs safety, and, in some cases, legally, even within the Information Assurance domain we would expect "people risk" to become an increasing concern. When we add emerging behaviours into the concept of digital risk we are creating an even larger gulf between expectations of responsible practice and the reality of this.

Referring back to the BIS (2014) survey, there are two emergent "threats" that come strongly from the report – social media/internet issues and also mobile technology, so we have at least some acknowledgement by industry that these are emerging issues. At least 38% of companies in the survey already said they had some form of countermeasure in place to address concerns over social media, although the majority looked simply to block access, something that perhaps does not acknowledge the breadth of risk, and the accessibility of the technology outside of the workplace. We will explore the complexity of these issues in more detail in chapter 3, but by way of introduction to these issues we will conclude this chapter by exploring what "risk" might be introduced through the simple introduction of social media in the workplace.

The growth and adoption of social media over the last ten years has been unprecedented when compared to the adoption of any other form of social technology. The Pew Internet Research Centre reports that 74% of adults who are online are using some form of social media[5]. While, as the name suggests, most use of these technologies are used for social purposes – it is inevitable that something people are so used to using, and interacting with, will have some spill over into the workplace. At a macro level, there is a question around whether it is a fair expectation of an employee to be able to use social media at work – after all, this is not something they need to use to perform their job. As can be seen from the BIS (2014) survey, many organisations do try to prevent access to social media via their own ICT infrastructure through blocking or filtering and, in some cases, developing policies around access via mobile devices. However, it would be technically difficult, and potentially an abuse of an individual's human rights, to demand an employee could not access social media at work, or ban an employee from engaging with social media at all. Therefore, it is important for organisations to recognise the emerging issues that arise from employees engaging with social media. Table 2 defines a number of corporate risks associated with employees' use of social media. It is not intended to be a definitive list – this would be a very difficult thing to do given the constantly evolving nature of social media and the frequent introduction of new forms – but an indicative one to provide an illustration of the breadth of issues that can arise if we incorporate social behaviours into digital risk:

Risk	**For Example**
Recruitment	The temptation to look at potential new recruits on social media to prejudge them regarding suitability for new positions
Liability for acts or views of employees	If an employee uses a social media platform to be abusive about another employee
Liability for treatment of employees	If an employee complains that a colleague/manager has been using social media to bully/harass
Reputation	If an employee uses a social media platform in an embarrassing, socially ambiguous, or litigious manner
Breaches of confidentiality	If an employee uses a social media platform to talk about work practices, colleagues, clients, etc.
IT security	If an employee uses social media to disclose information that might be used in an attack, for example, phishing.
Loss of productivity	If an employee is spending time on social media when they should be working
Privacy issues in monitoring use	If the organisation is monitoring Internet use on corporate infrastructure, is this disclosed to the employee?

Table 2.2 – Potential risks created by the use of social media

From this table we can see that social technology changes and extends what we traditionally see as digital risk. A key difference is that we no longer only have risks to IT assets. The range of impacts extends into areas such as reputation, human resource issues and also potentially litigation. Therefore countermeasures also have to be expanding in their scope – moving away from technical approaches to consider in more detail what can be captured in policy, and which policies should be expanded, what are the responsibilities of the employer for making employees aware of the potential for harm their behaviours may cause, what training should be in place, and so on. We also have to consider that in a number of cases, prevention is no longer a realistic option and therefore we have to reflect upon what an organisation might do to, for example, demonstrate due diligence.

The following chapter will extend the remit further, particularly exploring behaviours drawing from primary research with young people to demonstrate the emergence of technological normalisation and the need, within the digital risk context to contain this and provide adequate protection for both employer and employee.

3 Legal, Ethical and Moral Responses

In this chapter we further extend the concept of digital risk in the workplace to consider those issues not directly related to technologically per se, but from a wider social context facilitated by technology. It will consider these issues within the context of both legal response and moral reaction, and also explore the concept of *normalisation through digital technology* – the concept that some things are viewed as more acceptable if facilitated via digital technology than if it is conducted in an "offline" manner.

This chapter will draw on primary data based upon many conversations with young people, both secondary school and university students. These have been the result of much fieldwork with young people, working with them in schools to discuss how digital technology affects their lives and how these behaviours may cause issues in the workplace. This chapter also allows us to explore questions of legality and morality along with young peoples' awareness of the acceptability of their acts, the education and awareness they have, and how they develop resilience in the absence of education. Finally this chapter provides an exploration of issues with those who might be considered "offenders", and whether they even recognise their behaviours as either unacceptable or illegal.

The notion of legality is an interesting one in this area and while this text should not be seen as a legal proposition, it should be acknowledged that case law in both the UK and US can demonstrate the problems faced by companies in protecting themselves and their employees. We have already discussed the dismissal of three high court judges in the UK after they were caught accessing pornography at work. We also mentioned the Andrews case in Canada, which is worthy of further exploration because it does demonstrate a particularly interesting concept – that moral unacceptability does not necessarily mean adequate protection in the workplace, particularly when moral reaction can be ambiguous.

In this case an employee was dismissed for "Time Theft" – after many years unblemished service he was caught spending, over a long period of time, significant amounts of his working day accessing the Internet using work provided equipment, and some of that access was for sexually explicit material. However, at adjudication the defendant argued that while he was accessing the Internet, it could not be demonstrated that his work had suffered and after such a long period of flawless service, dismissal was a disproportionate response. The adjudicator agreed and he was reinstated (although not provided with back pay for the period of time he was accessing pornographic sites). This seems utterly counterintuitive for a moral perspective – few would agree that employees should be allowed to access pornography at work, using work equipment. However, as the employer failed to demonstrate the reason for dismissal in evidence, their management of this particular digital risk failed.

Further cases in the UK have highlighted the ambiguity of a number of issues around the "control" of social media and responsibly in the workplace, and a few interesting cases are illustrated below:

- **Taylor vs Somerfield** – In this case an employee of Somerfield posted a video of colleagues fighting with plastic bags stuffed with further plastic bags. While the video was posted on YouTube, it was only available for 3 days, and was viewed 8 times (including 3 views by managers at Somerfield). While Mr Taylor was dismissed for "gross misconduct for posting inappropriate film footage onto the YouTube website which brought the company into disrepute", his was reinstated on appeal as the company could not demonstrate disrepute as the video had received so few views.[6]
- **Crisp vs Apple** – However, in this case, Mr Crisp was posting derogatory comments specifically about his employer on Facebook, and subsequently dismissed. While he appealed and took the case to court, the judgement was upheld as Mr Crisp had been made aware of Acceptable Usage Policies where specific mention was made to not do anything on social media that would harm the company's image.[7]
- **Smith vs Trafford Housing Trust** – This case highlights that social media should still be viewed as a predominantly social platform, which cannot be used by employers to control the views of employees outside of the workplace. Mr Smith was a Facebook user whose profile said he was a manager at the Trafford Housing Trust and he was also friends with a lot of other employees at the organisation. Mr Smith posted a link to a news article about the impending legalisation of gay marriage in the UK, stating that it was "an equality too far". Mr Smith continues in discussion with two work colleagues who then reported his posting to their employer. Trafford Housing Trust undertook disciplinary proceedings and found Mr Smith guilty of gross misconduct – rather than dismissing him he was demoted to what would amount to a 40% pay decrease over 2 years. However, Mr Smith challenged this is court claiming breach of contract, which the court found to be true, stating that the postings were clearly personal and not representative of the Trust, and that just because work colleagues were friends this did not mean workplace rules could be applied, as one could view this control as an attempt to hamper Freedom of Expression.[8]
- **Gill v SAS Ground Services Ltd** – Nonetheless, in this case a more straightforward, and increasingly familiar case of an employee claiming to be off work ill was found to be posting activities on social media that would not reflect being at home ill. In this case Ms Gill was off sick while posting about attending, and participating London Fashion week, with comments about auditioning models and arranging a show. In this case the courts upheld dismissal on the grounds of gross misconduct.[9]

From these cases we can see that even at a straightforward level (i.e. postings on social media platforms) employers have to take care in protecting reputation verses policing the behaviour of employees outside of the workplace environment. It is not enough to decide anything an employee posts on social media reflects on their employment, they need to demonstrate that link and, as demonstrated in the case of Crisp vs Apple, can protect themselves considerably through the use of applicable policies. However, we can also see employers over reaching with their control over employees, with a number of articles around employers asking potential new employees to surrender their social media logins so they can be vetted[10]. While this might be viewed as a way of managing digital risk for organisations, particularly around reputational issues, it is beginning to be outlawed in some US and Canadian states due to human rights violations[11].

Another area that organisations need to be mindful of is the role of social media and digital technology in its use in workplace abuse and harassment. Online bullying is certainly nothing new but the focus is usually the impact among young people (for example, Jones, Mitchell and Finkelhor 2013). However, it is increasingly acknowledged as a workplace risk and its impacts can be significant. Work carried out to explore early cyberbullying issues among teachers (Phippen 2011) showed that those within the education sector were often subject to abuse online (reported statistics state 36% of 350 respondents had been subjected to some level of online abuse), and while the majority of abuse was from pupils, in around 10% of cases victims reported abuse from colleagues. The impact of such cannot be underestimated, as described in both the above research and also subsequently in research for ACASS (2012), which showed severe impacts such as depression and in a small number of cases suicidal tendencies. It is therefore important that companies recognise firstly that their employees may be subjected to abuse by colleagues in online environments but also that they may be providing the facilities for abuse to take place. They need to demonstrate, through policy (such as bullying or acceptable usage) and training, both an awareness of the issues and also the reporting routes for victims and incident response mechanisms.

Awareness of harassment and the right to protection is something that arises in a lot of our work – in a lot of cases, discussions with subjects have highlighted that, while they view behaviours they are subjected to as upsetting or unpleasant, they are not aware that they do not have to put up with such and they have a right to protection from abuse or harassment.

This is something that we encounter more when digital technology is involved and can be clearly highlighted from a quote from a 20 year old female who worked in a predominantly male environment – oil refineries:

"I work on refineries and many men cheat on their partners and due to me being the only under 40 female on the site for 800 guys many filtered with me sending pics of cock"

At face value this is an astonishing thing to say – primarily because this is an individual who is regularly subject to harassment in the workplace in the form of images of her workmates genitals being sent to her, by those colleagues. However, on further analysis what is more shocking about this person's comment is that she is legitimising this as "flirting" – an example of normalisation through technology. Would the same individual view this as flirting if her colleagues were walking into her office to expose themselves? It seems from the quote that, because the image is delivered via technology, it is ok.

Sexual harassment practices, in particular, seem, from our conversations, to be something that is normalised via technology. A frequent comment from teenagers and students in our experience is the idea that there is nothing wrong with receiving a message via technology from a friend or acquaintance asking them to take an indecent image of themselves and send it to them (commonly referred to as sexting). While we might view this as a youth practice, it is clear from many news stories (a recent one referring to a UK Member of Parliament[12]) this is certainly not the case. Again, to take the offline version of this, when we discuss this practice with young people we often ask whether it would be acceptable to ask a colleague face to face to take an image of themselves naked and send it to them? Generally the response to this inquiry is that it is unacceptable, which does beg the question why is it then viewed as acceptable if the request comes via digital means?

Also, reflecting on the act from the "offender's" perspective, it is interesting to also note that in many cases those requesting an image, or volunteering one without prompting, equally do not see that they are doing anything wrong and this is something that has become "the norm" among their peer group. While ignorance is certainly not a defence, returning the emergence of "digital natives" into the workforce we need to be aware that we might not just need to protect victims but also make it aware among those who might engage with such practices that it is unacceptable and, potentially, illegal.

A particularly concerning aspect from our work is that, in lieu of any education, awareness or training around the acceptability or otherwise of such behaviours, along with such practices as sending pornographic images and similar as "a joke, individuals develop their own coping and resilience mechanisms. And such responses are extremely variable, from those who "just put up with it", to those who will escalate issues in equally risky ways (for example, forwarding received images to others) to those who will respond with abuse in return.

Certainly from our experiences in speaking with young people a lot of these behaviours are hidden behind the general veil of "banter" or "pranks". It is interesting to note that a lot of public reaction to these issues shares a similar view. A recent prosecution of a student in the UK highlighted this. In this particular case[13] a student, drunk at a party decided to get his friend to record him placing his genitals on the face of a sleeping female. The victim became aware of the video when the student's friend was sharing it with work colleagues. The victim quite rightly viewed this as sexual assault and the offender was sentenced to nine months in prison, but the public reaction was, at times, one of shock at the sentence, illustrated by one comment taken from the Daily Mail reporting of the story[14]:

"The video this idiot boys so called friend took will have been used as evidence? 9 months jail is crazy – not much less than gun freak killer Pistorius got. But this silly wretch didn't rape the girl, and likely both drunk, as students tend to get. Probation would have been better idea."

However, while the above quote might show some public response to such behaviour, in a workplace context it is important that organisations are aware of such practices and the possibility of them being conducted by employees. It is also important that they have measures in place, through policy, training, and similar, to protect their staff from the potential impact of such and to provide robust responses to demonstrate due diligence and ensure they cannot be accused of complicity in providing environments for abuse.

In concluding this exploration of the extent of digital risk in the workplace, we can see it can cover a wide range of issues, from those traditionally in the Information Assurance domain to some that are clearly beyond such data protection practices. However, it is also important to note that this is not an area that stands still and risk assessments should also consider what is emerging in practice. Again, from our own experiences in the education sector, the argument that staff receive training every few years (which we have heard on several occasions) is not adequate. With the constant emergence of new social technologies it is important that organisations are aware that these issues do not stand still and they need to ensure risk assessment practice, policy and training can be appropriately updated to reflect new trends and behaviours.

In the second half of this text, we explore approaches that organisations can adopt to consider these in a risk management framework, in order to protect both their employees and themselves for the potential for harm, in whatever form, which might result.

4 Elements of Effective Digital Risk Management

Risk management is a comparatively new discipline. Although humankind has been managing risk for thousands of years, it is only in the last few decades that we have chosen to develop formalised risk management frameworks.

Digital risk management has come a long way in this time and, as we explained in chapter 2, IT security standards have been in place since the 1990s. It is not therefore our intension to replicate the contents of these standards, since they are already well known and widely communicated. Rather we emphasise the elements of effective digital risk management that are not so well reflected in the existing standards.

Despite their widespread use and undoubted value in relation to some of the basics of digital risk management, the existing IT security standards have been criticised for being both generic in scope and based on (non-validated) common practice (Siponen and Willison, 2009). It is also the case that digital risk management has fast moved beyond 'simple' IT security issues to encompass other factors such as online behaviours (e.g. bullying) and reputation issues. These latter issues (a focus on common practices relating almost exclusively to IT security) are particularly problematic in today's digital risk environment, where the techno-centric foundations of IT security practice have not necessarily caught up with the fact that digital risk management is as much about understanding and managing people as it is about developing every more sophisticated (and complicated) hardware and software solutions (see, for example, Coles-Kemp (2009).

Therefore, one essential element of effective digital risk management is to recognise that technical hardware/software solutions are not a panacea. As Bunker (2012, p. 20) points out the encryption of a laptop or USB stick might appear to solve the problem of data theft in the event that such devices are lost, but what if the password for a device is taped to it, because the user could not remember all their passwords? IT security professionals might claim that such an error of judgement is not their problem and that they did their job by encrypting the device. However the data has still been lost, so such a defence is rather hollow. It would be better if IT security professionals could cross the "digital divide" between themselves and users (Albrechtsen and Hovden 2009, p. 476) to take a holistic approach and address both the technical and the human elements of the problem. Only then can the data in question truly be secure.

In order to balance the human and technical elements of the digital world it is helpful to think of digital risk management as a socio-technical system, as illustrated in Figure 4.1 (Coles-Kemp 2009; Kraemer et al 2009). Such a system recognises and seeks to manage the interactions, whether intentional or not, that exist between the people and technology (hardware and software, as well as organisational structures, processes and procedures) that are found within organisations. In this context digital risk management is no longer isolated to the achievement of technical excellence through the implementation of formal (mechanistic) IT security frameworks or the implementation of state of the art technical controls (firewalls, encryption, etc.). Instead it becomes one of achieving joint optimisation between the social and the technical. In this context technical excellence may no longer be necessary or desirable where it might interact in damaging ways with the people element of the equation (remember the laptop encryption example). Equally it may well be that changes to the behaviours and attitudes of the people within an organisation may prove a more effective means to control IT security risks than technical innovation.

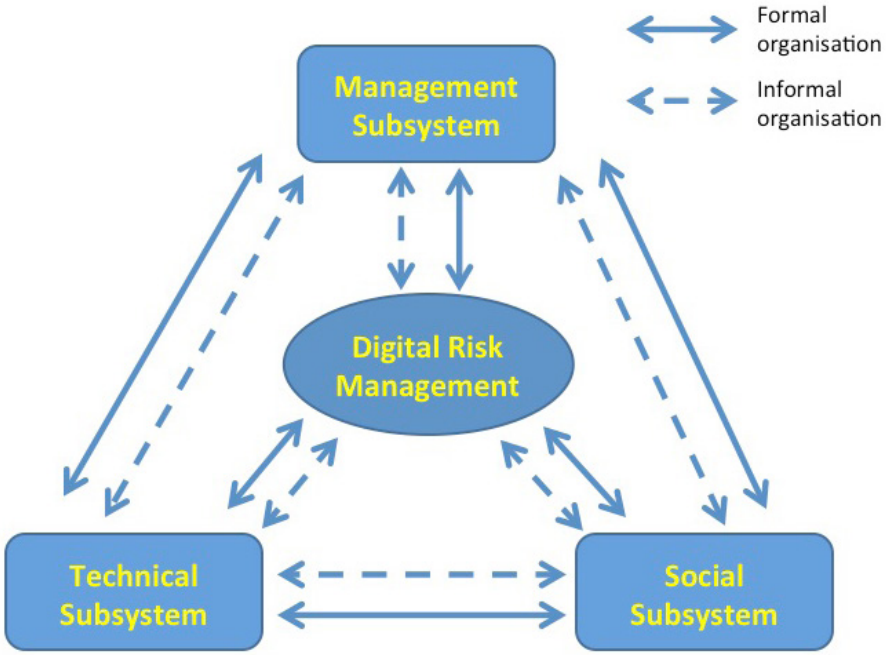

Diagram 4.1: Digital Risk Management within a Sociotechnical System

A further essential, but often under-emphasised, element of effective digital risk management is to ensure that it forms part of a wider enterprise risk management framework. Some practitioners might well prefer to believe that digital risks are unique and should be identified, assessed and controlled outside of other management considerations. However with organisations increasingly reliant on digital systems for every aspect of their strategy and operations, this silo perspective is increasingly outmoded.

Diagram 4.2: An Enterprise-Wide Approach to Digital Risk Management

Effective digital risk management within an enterprise-wide perspective reflects the operational and strategic aspects of digital risks. From an operational aspect digital risk events can clearly affect the cost, efficiency and continuity of an organisation's operations. However they may also have a broader strategic impact, either where their operational effects are so large so as to affect the achievement of an organisation's strategic objectives, or where they impact on an organisation's stakeholders. In the case of the latter it may well be that the operational effects of an event are relatively minor, yet stakeholders may still be adversely affected and an organisation's reputation may well suffer as a result.

A good example of this is the case of Nationwide Building Society, who in November 2006 lost a laptop that contained potentially sensitive customer information (though there is no evidence that any of this information was ever mis-used). The loss of the laptop did not, in itself, have any effect on the cost, efficiently or continuity of Nationwide's operations and did not directly affect customer service. However Nationwide was still fined £980,000 by the UK Financial Services Authority for inadequate IT security procedures (it took 3 weeks for the building society to investigate the theft and to inform customers of the loss of their information) and the affair significantly tarnished the reputation of an organisation that has always prided itself in excellent customer service[15].

The Nationwide case also illustrates the dynamic nature of digital risks, which are becoming increasingly difficult to manage using standard risk management techniques, such as risk registers or risk and control self-assessments (RCSAs). The Nationwide used such tools and had identified and assessed the risk of data loss, yet still failed to respond to the perceived significance of lost customer data and paid a heavy financial and reputation penalty as a result.

However that does not mean that digital risks are unmanageable. While stakeholder reactions to digital risk events may be hard to predict, it is not impossible to do so. Equally the strategies and techniques that are used by hackers and other malicious online participants can be predicted and managed to a degree. Though to succeed alternative risk management tools and techniques are required.

Kaplan and Mikes (2012) provide an excellent framework which can be used to support the management of digital risks on an enterprise basis. Although their framework was not explicitly designed for digital risks it is just as applicable in this context as for any other area of risk.

Kaplan and Mikes distinguish between three primary categories of enterprise risk, each of which is a potential source of digital risk. Table 4.1 adapts and builds on Kaplan and Mike's approach to provide a new framework for thinking about digital risks.

Primary Risk Category	Description	Example Digital Risks
Preventable (Operational) Risks	Internal risks that derive from the day to day operations of an organisation	• Hardware and software system failures • Internal breaches of procedure • Loss of data • Online bullying
Strategic Risks	Risks that are taken for a strategic return (profit, market share, etc.) or which may significantly affect the achievement of an organisation's strategic objectives	• Hardware and software systems development (e.g. the failed implementation of a new system) • Regulatory breaches (e.g. data protection) • Reputation risks (e.g. stemming from loss of data)
External Risks	Risks from the external environment (political, economic, social, etc.)	• External hacking and denial of service attacks • Theft of data

Table 4.1 Risk categories from Kaplan and Mikes (2012)

Kaplan and Mikes then go onto explain that each of these primary categories of risk requires a different type of risk management response in terms of assessment and control. So, just because a specific assessment or control tool may work for one risk category, does not mean that it will work elsewhere. Table 2 highlights some of the tools that can be applied to these three categories.

Primary Risk Category and Risk Management Objectives	Common Assessment Tools	Common Control Tools
Preventable (Operational) Risks Objective is to reduce the probability and impact of these risks, where it is cost effective to do so	Control effectiveness assessments (e.g. Control Self Assessments) Internal audit reports Probabilistic risk models (statistical analysis of loss data) Risk Registers	Business continuity plans Codes of conduct Data backup Policies and procedures Risk (IT security) culture management Staff training
Strategic Risks These risks are actively taken to achieve strategic objectives. Objective is to increase (reduce) the potential and scale of any positive (negative) outcomes	Probabilistic risk models (statistical analysis of profit and loss data) Probability/impact risk and opportunity maps Risk metric scorecards Risk workshops (utilising expert judgement)	Compliance management Programme management Media relations strategy
External Risks The probability of external risk events are difficult to reduce, hence the primary objective is to reduce the impact of such events	Tail risk assessments and stress testing Scenario planning War gaming (assessing vulnerability to external attacks)	Business continuity plans Data backup Firewalls Penetration testing

Table 4.2 Controls for Kaplan and Mikes (2012) risk categories

It is imperative that digital risk management professionals recognise these three distinct sources of digital risk (operational, strategic and external) and ensure that they have in place tools and techniques to support the assessment and control of each. As should be apparent from Table 4.2, this will involve utilising assessment and control strategies that may be unfamiliar to some digital risk professionals, especially those with a background in the technical aspects of IT security. However a balanced approach is imperative, in chapters five and six we will explore this issue further.

5 Assessing Digital Risk for Anticipation and Resilience

In this chapter we consider some of the strategies that can be used by organisations to assess digital risks, some more familiar than others. The basis for our approach rests on a key philosophical question in risk assessment, the extent to which risks can be anticipated and whether it is possible to assess an organisation's resilience to unanticipated events (which can be more common in a dynamic field like digital risk).

A key objective in risk assessment is to anticipate the potential for risk events and in so doing estimate both the probability of such events and their impacts. To achieve this time and effort is spent both in predicting the potential causes of risk events and in understanding their effects, should these risk events 'crystallise'. A difficult exercise at any time since most risk events are the sum of multiple causes (e.g. a wide variety of technical or human failures, external events, etc.) and can result in a range of effects (financial, reputation, business interruption, etc.), which may be further influenced by a complex array of control and recovery measures, as illustrated by diagram 5.1.

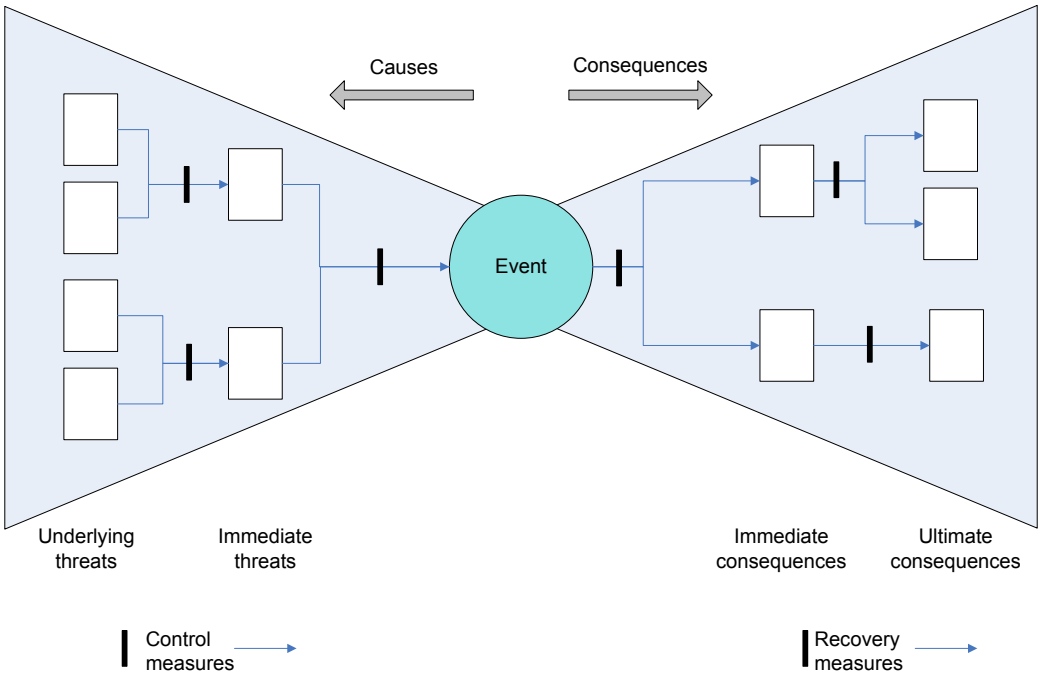

Diagram 5.1: The Cause, Event and Effect Chain

Given the complex array of causes and effects that may be associated with a particular risk event it is often not possible to anticipate every possible risk event. Even where an event is known to be a possibility, the full cause-effect chain may not be fully understood, meaning that the probability and/or impact of the event in question are under-estimated. In such circumstances it is necessary to embrace a further objective for risk assessment, the evaluation of an organisation's resilience to risk. Diagram 5.2 illustrates the key differences between assessing for anticipation versus resilience.

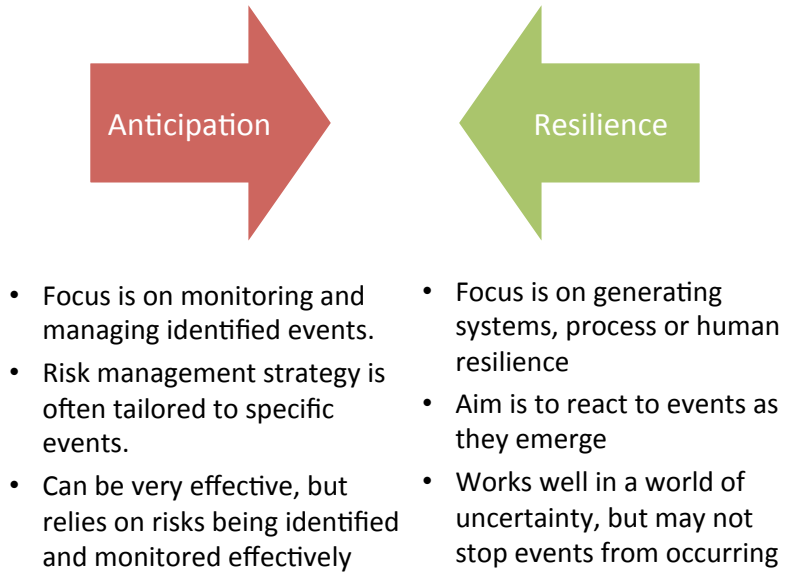

Diagram 5.2: Assessing for Anticipation Versus Resilience

In the ever changing risk landscape that characterises digital risk, where new technologies and social attitudes are constantly evolving and the legal environment can be equally uncertain, organisations will, from time to time, encounter causes, events and effects that they had not anticipated. The people risks associated with the emergence of "Digital Natives", are a good example of this (see chapter two), as are the legal cases outlined in chapter three.

Although it may be impossible to fully anticipate every digital risk event, much can still be done to assess the probability and impact of such events. Table 5.1 below highlights some of the techniques that can be used to support the anticipation of digital risk events and their associated causes and effects. Many of these techniques can be combined for greater effect. For example, a workshop might be used to support the use of a risk matrix or the completion of a bow tie analysis, equally a risk register might incorporate a control self-assessment.

Technique	**Description**
Audits and Inspections	'Physical' inspections of technical controls and audits of compliance with established policies and procedures. For example an on-site inspection of a key IT processing site.
Bow Tie Analysis	The structured analysis of cause, event and effect. Bow tie analysis will typically cover underlying and immediate causes, as well as short and long term effects. Controls may also be incorporated to understand how existing controls may help to mitigate specific causes and effects. This could include an analysis of the causes and effects of hacking attacks, cyber bullying, etc.
Control Self Assessments	A structured mechanism for assessing control effectiveness against agreed risk events. May include the assessment of individual controls, as well as the overall control environment for the risk event in question – in terms of both its design and implementation. Assessment is typically performed by the individual or individuals that are directly responsible for managing the relevant risk event. This tool can be applied to the assessment of almost all cyber risk events.
Fault Trees and Event Trees	Diagrammatic technique for exploring the sequence of 'faults' (i.e. causes) that must occur in order for a given risk event to happen (fault trees) or the sequence of effects that may follow a given risk event (event trees). Can be qualitative or quantitative in nature. Fault trees are effectively the same as 'root cause analysis'. Fault trees could be used to assess the root causes of specific types of hacking attack, while event trees can be used to investigate the potential effects of actual cyber risk events.
Flowcharts and Dependency Analysis	Analysis of systems and processes to identify potential weaknesses (e.g. the potential human error) and interdependencies (e.g. between core IT systems, where the failure of one system may affect several others).
HAZOP and SWIFT Analysis	Structured team-based qualitative analyses of systems and processes. Hazard and Operability Studies (HAZOP) explore the operating of complex processes to determine potential hazards that may affect the efficient/cost effective operation of these processes or the health and wellbeing of those operating these systems and processes. Structured What If Techniques (SWIFT) is a similar form of analysis that uses sets of prompt words to assess risks in a structured 'what if' manner. SWIFT uses a checklist approach to look for pertinent deviations from normal operation, and considers a system as a whole or in larger process sections than HAZOP.

Risk and Control Indicators	Risk indicators are metrics that provide information on the level of exposure to a given risk which the organisation has at a particular point in time. Risk indicators may provide information on the current significance of a particular cause or the likely scale of the effects of a risk event, should one occur. Examples might include the number of attempted hacking attacks, external reports on virus threats, etc. Control indicators are metrics that provide quantitative information on the current effectiveness of a given control. Examples include number of reported policy breaches, the frequency of data back up and any delays in software patching or essential IT security training.
Risk Matrices (Probability and Impact Assessments)	Use of ordinal (scaled) probability and impact assessments plotted on a risk matrix or heat map to assess the risk. Common scales include 3x3 and 5x5 probability and impact matrices.
Risk Registers	Register of potential risks to provide a summary of the overall risk profile for a given business area, activity or process/system. Will usually include a description of the risk and an ordinal (scaled) assessment of probability and impact. May also include information on potential causes and effects, as well as an assessment of available controls.
Risk Workshops	Involves the collection and sharing of knowledge and experience of relevant 'experts'. Will include the discussion of causes, events and effects that could impact on strategic objectives, stakeholder expectations or key operational dependencies. It is common to support these discussions with a structured approach to the identification and evaluation of this, for example: An agreed risk categorisation framework, SWOT Analysis (consideration of Strengths, Weaknesses, Opportunities, Threats) PESTLE Analysis (consideration of Political, Economic, Social, Technological, Legal and Environmental threats)
Scenario Analysis	The analysis of potential future events (usually more extreme adverse events) by considering alternative possible outcomes ranging in severity. Can be applied to investigate the occurrence of multiple future events and a variety of potential causes and effects. May involve the estimation of maximum possible and maximum probable loss, or may be purely qualitative. Historical information may be used to support the development of a scenario, but the emphasis is very much forward looking. The aim being to examine future trends and turning points (e.g. the emergence of new causes/effects or potential new control failures). Usually completed within a workshop environment, utilising the judgement of multiple experts from diverse backgrounds. This kind of analysis can be used for all kinds of cyber risk events, but especially more serious events (such as a major denial of service attack, or the death of an employee due to cyber bullying).
Statistical Risk Models	The use of statistical techniques to help explore complex risks with multiple inputs and a range of potential financial outcomes. Usually involves the development of computer models.

Stress Testing	A form of particularly intense or thorough testing used to determine the significance of a given risk factor (whether cause or effect related) or the effectiveness of a particular control. It involves testing beyond normal operational capacity, often to a breaking point, in order to observe the results.
Voting Mechanisms	The use of opinion-polls and questionnaires to assess the probability and impact of a given risk event. Relevant staff members (IT experts, business managers, etc.) are asked to individually rank a particular risk, or set of risks in terms of probability and impact and the results are compared to determine the level of consensus. Where significant differences are found further discussion may be required.

Table 5.1: Techniques for Anticipating Digital Risks

The assessment of an organisation's resilience to unknown risk events and or unforeseen causes and effects might seem impossible. However the trick is not to look directly for these specific causes, events or effects, but rather to consider some of the more fundamental elements of resilience. Notably:

1. An organisation's ability to detect unexpected causes, events or effects, preferably before they have significant (averse) consequences.
2. An organisation's willingness to accept and respond to unexpected causes, events and effects.
3. An organisation's ability to recover quickly and to learn from unexpected causes, events or effects.

One field of research that provides a mechanism for assessing resilience is the work that has been conducted into 'high reliability organisations' or 'HROs'. This research, which was completed following detailed analyses of a range of (resilient and much less resilient) organisations, provides significant practical insight into assessing resilience.

Diagram 5.3: Characteristics of Resilient Organisations

Diagram 5.3 is adapted from the work of Karl Weick and Kathleen Sutcliffe (Weick and Sutcliffe, 2007), who have done much to improve the ability of organisations to manage the unexpected. These characteristics extend the fundamental elements of resilience outlined above, to provide a more detailed explanation of the factors which can determine an organisation's resilience to unexpected digital risk events[16].

The task for organisations is then to assess these elements so that they can determine how resilient they are. Weick and Sutcliffe (2007, ch 5) suggest using an audit approach, via the analysis of attitudinal statements that are circulated to as large a number of employees as possible, who then score from 1–3 the extent to which they agree with a range of statements. Such an approach has potential merit, but can be cumbersome to implement and the responses are prone to bias. As an alternative we offer an evidence based, binary questionnaire approach to support the assessment of digital risk resilience within organisations (see Appendix A). This questionnaire draws on Weick and Sutcliffe's work, but is reduced to a series of yes/no questions coupled with the addition of a free text evidence field. The questionnaire covers a range of key social, technical and managerial factors which can influence an organisation's resilience to digital risk.

We suggest that the questionnaire is presented to two groups and the results compared:

- The senior managers within an organisation, up to and including executive directors.
- Risk and control professionals. Including enterprise risk managers, internal audit and compliance staff and IT security managers.

It is important that respondents complete the open text field when they answer yes to a particular question. The aim of this field is to provide evidence to support their attitudinal responses and to highlight their personal level of engagement in maintaining a resilient organisation. To ensure openness and frankness these questionnaires may of course be returned anonymously, providing it is possible to distinguish between the abovementioned two groups of respondents.

Finally no chapter of the assessment of digital risks would be complete without a discussion on developments in the analysis of 'big data'. This field is still comparatively youthful, but offers a lot of potential for the assessment of digital risks in the future. In particular the use of big data techniques may well help to improve our ability to anticipate future digital risks by highlighting emerging social trends. They may also highlight potentially unknown correlations between the causes and effects of digital risk events.

In our modern world exceptionally large datasets are becoming more and more common. Such data offers a wealth of potential information; however it is often difficult to process using traditional relational databases and/or standard statistical techniques. Instead big data analysis requires the use of inductive and or non-linear data analysis techniques such as crowdsourcing, genetic algorithms, machine learning, simulation and visualisation (use of images such as a 'word clouds').

A detailed investigation into big data risk assessment techniques for digital risks is beyond the scope of this book[17]. However to help those readers interested in this field the table below highlights some of the commercial developments in the big data analysis of digital risk events. Note that these websites are simply provided as examples of recent developments. No recommendation of the products and services which are on offer should be implied. In this field new products and services are emerging all the time and those organisations interested in using commercial big data products should carefully explore the available options.

Organisation	Description	Website
EMC[2]	Information management and security organisation. Offers a range of big data solutions. Subsidiary RSA Archer offers risk analysis software.	http://www.emc.com/big-data/index.htm
Google BigQuery	Cloud based big data analysis tool from Google. Not specific to digital risk assessment, but easy to access and has pay as you go pricing. Includes a prediction tool (Prediction API)	https://cloud.google.com/bigquery/?gclid=CMj198LynMECFSbmwgodszoAcg
IBM InfoSphere	IBM offers a range of big data software tools, including the InfoSphere range of big data analysis and warehousing products.	http://www-03.ibm.com/software/products/en/category/bigdata
MetricSteam	Risk analysis and management service provider. Offers a range of 'risk intelligence' solutions which make use of big data analysis.	http://www.metricstream.com/microsite/bigdata/
Parker Fitzgerald	Example of a supplier of 'digital risk assessment and management solutions' which utilises big data analysis. Focuses on the financial services sector.	http://parker-fitzgerald.com/what-we-do/digital-risk-solutions/
SAS	Data management and analysis service provider. Offers a range of software and consultancy products including risk assessment software and bespoke big data analysis via 'Answers from SAS'.	http://www.sas.com/en_gb/home.html
SPLUNK	"offers the leading platform for Operational Intelligence"	http://www.splunk.com/

Table 5.2: Commercial Developments in Big Data

6 Controlling Digital Risk: The Levers of Control

A primary objective in the management of digital risk is to help prevent, detect or at least mitigate and ultimately recover from the effects of digital risk events. To that end almost all organisations will have some controls in place to help manage their digital risks, but do they necessarily have the right mix of controls to ensure the most effective control environment? In particular organisations need a diverse suite of controls that can deal effectively with both technical and people related digital risks.

In this chapter we will explore mechanisms for controlling digital risk. However rather than getting lost in the detail of all the different tools and techniques that can be used, our intension is to provide a framework to help better organise the control environments of organisations and improve their effectiveness. In so doing we provide a framework for the control of digital risks that builds on the extended notion of digital risk provided in chapter two.

In simple terms the control of digital risks will involve a range of preventive (e.g. access controls), detective (e.g. virus scanning), and corrective controls (e.g. file backup procedures) to help deal with the causes and effects of digital risk events. A good mix of these types of control will help to ensure that an organisation can deal with both anticipated events and have a degree of resilience in place to cope with the unexpected (corrective controls such as file backup procedures should work whether the event that led to a loss of data was anticipated or not).

However following on from Chapters 4 and 5, if an organisation is to adopt a sociotechnical approach to digital risk management, to ensure that it can deal with both people and technical digital risks, then its control environment must involve a balance between the 'hard' technical controls that characterise the field (e.g. access controls or firewalls) with a comprehensive range of more people centric 'soft' controls, such as creating an appropriate digital risk culture. In so doing we resurrect and extend a long established but underutilised framework for structuring risk control activities: Simons' (1999) 'Levers of Control'.

Simons (1999) provides four primary levers for the control of organisations. These levers can each be used to help manage the causes of risk events, and at times may also be used to mitigate their effects (through the speedy discovery of an emerging risk event, for example). Although Simons' levers were not developed with digital risk in mind, they provide a useful mechanism for thinking about the mix of technical and more people oriented mechanisms that should be used to control digital risks. To make it more relevant to digital risk management we extend Simons' work to include a 5th lever – that of continuity systems, which are vitally important when dealing with the unexpected and highly disruptive nature of digital risk events. Table 6.1 explains these levers and provides some example digital risk controls to illustrate each category.

Levers of Control	Description	Example Digital Risk Controls
Belief Systems	Controls which directly influence the beliefs and values of employees, to ensure that these are not potentially destructive and are consistent with the mission and values of the organisation	• Tone from the top, in relation to the value placed on digital risk management. • Value lead performance reviews. • Digital risk training and awareness campaigns designed to influence beliefs and values.
Boundary Systems	Controls which limit the actions and behaviours of employees and other relevant actors (e.g. external hackers). Includes controls which make clear the limits of acceptable behaviour.	• Acceptable use policies and relevant codes of conduct (in relation to the digital environment). • Access controls and firewalls. • Data encryption.
Diagnostic Control Systems	Monitoring tools to help diagnose potential vulnerabilities to risk and the likely crystallisation of risk events.	• System performance monitoring • Penetration testing • Monitoring and reporting of other relevant key risk and control indicators
Interactive Control Systems	Controls that help to encourage debate and discussion on risk and stimulate learning (e.g. learning from past events)	• Digital risk event and near miss analysis and reporting • Open communication arrangements including a 'no-blame' approach to digital risk events
Continuity Systems	Mechanisms to maintain the continuity of an organisation and facilitate a rapid recovery post event.	• Server/disk mirroring • Data backup • Business continuity plans • Media relations strategy

Table 6.1 Simons' Levers of Control Applied to Digital Risk Management

An effective control environment for digital risk should incorporate each of these levers. The specific controls that are used and the emphasis allocated to a specific lever may well vary over time and almost certainly will vary by the type of digital risk in question. However it will be rare to encounter a situation that does not demand a mix of controls from each lever.

Digital risk professionals may feel less comfortable dealing with some of the softer people orientated levers of control outlined above, notably 'Belief Systems' and 'Interactive Control Systems'. Indeed the majority of established digital risk controls fall within the realms of 'Boundary Systems', 'Diagnostic Control Systems' and 'Continuity Systems', which tend to involve the use of technical controls. These technical controls are clearly very important in managing digital risk, but they are no panacea. The use of softer, more people orientated controls are equally important and must not be ignored.

To help make better use of belief and interactive control systems digital risk managers should develop much closer relationships with their organisation's Human Resources function. HR professionals are often experts in the softer elements of risk control (such as the management of organisational cultures) and have access to a range of specialist tools and techniques that can be used to support the management of digital risks. For example, they may be able to adapt the organisation's recruitment procedures to help filter out employees that could expose the organisation to a high level of digital risk (e.g. by social media due diligence, such as looking at an applicant's public web profile). Also the induction process could be used both to raise awareness of digital risk issues and to ensure that policies and procedures are understood, including the implications for non-compliance.

HR professionals should also be able to support attempts to manage those aspects of an organisation's culture that might influence its digital risk exposures such as attitudes to IT security (see, for example: Da Veiga and Eloff, 2010; Ruighaver, et al 2007; Chia, et al 2003). An 'appropriate' IT security culture should help to reduce the risk of accidental and deliberate IT security loss events, by influencing the behaviours of employees. This is achieved via mechanisms which affect the way in which these employees perceive IT security risks and make decisions (e.g. control decisions) about both their own, and their organisation's, level of exposure.

There are many belief and interactive control systems that can be used to create an organisational culture which better supports the prevention, detection and correction of digital risk events. These mechanisms include: promoting security awareness through training and education initiatives; management styles and attitudes (the so called 'tone from the top'); performance reviews and performance related pay; disciplinary procedures; and recruitment procedures, amongst others. The precise mechanisms employed, along with their design, will tend to vary by organisation (there is no one size fits all approach to any form of organisational culture), though there are frameworks available to help organisations select an appropriate set of mechanisms (e.g. Da Veiga and Eloff, 2010).

In terms of establishing effective interactive control systems for digital risk the importance of two-way communication must also be emphasised. Here organisations should clearly ensure that they keep all relevant staff informed of the potential digital risks that they may encounter and significantly the implications of these risks to the organisation. However the other side of an effective communication system is information transfer from staff to the 'organisation'. Of particular importance here is encouraging staff to be open about their mistakes (e.g. accessing a virus infested web-site or sharing confidential information). In addition whistle blowing procedures can help to prevent less scrupulous staff from reporting errors. With the timely reporting and monitoring of incidents effective remedial action can be taken to limit any damage. In addition, lessons can be learned for the future, enabling new control strategies to be put in place.

7 Conclusions

In this short book, we have explored the growing problem of digital risk in the workplace, and how organisations might respond to the sorts of issues that arise and might be categorised as such.

While at first glance we might consider that the growth in digital behaviours that extend beyond the traditional remit of Information Assurance are a result of the emergence of a younger, more digitally engaged, workforce (referred to by some as "Digital Natives") we would argue that this is a simplistic interpretation of the blurring between social and workplace boundaries that have resulted from the advent of social media, mobile technology and readily available Internet facilitated services and that digital social behaviours, with potential workplace impact, are not purely in the realm of the younger aspects of the workforce. We need to bear in mind that employees of all age ranges are engaging in digital social technologies and their behaviours are adapting as a result of this adoption.

We used the recent case of High Court judges in the UK being dismissed for accessing pornography at work as a good example of both the breadth of workforce who might engage with "risky" digital behaviours in their workplace and also the breadth of issues that such behaviours introduce to the risk assessment practices at an organisation. In this simple case we introduced issues such as:

- the monitoring of Internet access and employee rights;
- the ethical interpretation of practices that are perfectly legal;
- defining policy to encapsulate digital behaviours at work;
- awareness raising and training at work to communicate corporate policy;
- the difference between "common sense" and due diligence in an organisational setting.

We propose an extension of the traditional domain of Information Assurance, which is generally focussed on risk caused by the application of digital technology to workplace processes and the protection of assets and data held by organisations. Companies need to consider a whole range of risk issues that are introduced through digital behaviours that are not specifically tied to organisational functions and processes, but may be conducted using their systems and technology and extend risk beyond traditional corporate and IA domains to areas such as reputation, litigation and due diligence. Consequently, organisational countermeasures equally need to be extended to consider what can be captured in policy, and which policies should be expanded, what responsibilities the employer has, and how it might protect both the organisation but also their employees from the potential harm that might result from digital behaviours.

We have also explored the grey area between legislative requirements and organisational response, and how legislation, while catching up with these sorts of behaviours, can sometimes struggle with the imprecise practice and outcomes of digital risk, particularly held against the social normalisation that sometimes occurs when behaviours manifest on a digital platform or device. We have illustrated this with a number of examples that are drawn from the field of harassment and sexual abuse, all of which seem to have blurred moral responses due to the digital nature of the abuse discussed – for example the sending of a digital image of someone's genitals to a colleague seemed, in one case described to be in some way acceptable (and legitimised by the victim) whereas an offline version of such would be clearly considered completely unacceptable.

All of these issues show the need to develop and update digital risk management and bring in leading edge thinking to help an organisation develop the tools to keep themselves and their employees protected by the growing portfolio of perils. One thing we believe is essential is that digital risk should not be treated as something 'special' and dealt with in a specialist manner. However, it is the very fact that digital risk can, while using technology as a vehicle for execution, cut across an organisation that they should be incorporated into a broader, corporate wide, risk management framework rather than a "digital risk" silo.

In incorporating into a digital risk management strategy, we present a number of tools to help with the categorisation, assessment and control of risk, as well as demonstrating due diligence. However, we also argue that these tools need to be incorporated within a socio-technical approach to risk management which acknowledges risk cannot just be controlled through policies and technology but through training, knowledge and understanding. A sociotechnical approach enables an organisation to deal with both the people and technological aspects of digital risk and the unexpected outcomes that can arise out of the complex nature of their interaction. It is important that the communication is a fundamental part of a digital risk management strategy along with the development of an appropriate *digital risk culture* that embraces all employees. Ultimately such an approach will reap far more benefits than a top down, policy driven approach.

Emerging technologies constantly introduce new potential social behaviours which can manifest in a workplace setting and also increasingly blur the boundaries between an employee's social and work life. A culture where the organisation learns from its employees means that they can anticipate potential emerging risks far more effectively than if this is an imposed strategy. What is clear from this exploration of this constantly evolving topic is that standing still is not going to ensure the adequate management of digital risk and organisations need to constantly update their knowledge in order to best manage the ever changing digital risks they are presented with. Is your organisation ready, willing and able to respond to these challenges?

References

Albrechtsen, E. and Hovden, J. (2009) "The information security digital divide between information security managers and users", Computers and Security, Vol. 28, 476–490.

BIS (2014) "Information security breaches survey", *Department for Business Information and Skills*, http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf

Bennett, S., Maton, K. and Kervin, L. (2008) "The 'Digital Natives' debate: a critical review of the evidence", *British Journal of Educational Technology*, Vol. 39, No. 5, 775–786.

Bunker, G. (2012) "Technology is not enough: taking a holistic view for information assurance", *Information Security Technical Report*, Vol. 17, 19–25.

Chia, P., Maynard, S., and Ruighaver, A. Eds. (2003) "Understanding organisational security culture" in *Information Systems: The Challenges of Theory and Practice*. Las Vegas, USA: Information Institute.

Coles-Kemp, L. (2009) "Information security management: an entangled research challenge", *Information Security Technical Report*, Vol. 14, pp. 181–185.

Cummings, R. (2002) "The evolution of information assurance" *Computer*, Vol. 35, No. 12, 65–72.

Da Veiga, A. and Eloff, J. (2010) "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29, 196–207.

Furnell, S. and Phippen, A. (2007) "Raising a generation at risk". http://www.bcs.org/content/ConWebDoc/10312

Howe, N. & Strauss, W. (2007) "The next 20 years: How consumer and workforce attitudes will evolve" *Harvard Business Review,* Vol. 85, No. 7/8, 41–52.

Jones, L.M., Mitchell, K.J., & Finkelhor, D. (2013). Online harassment in context: Trends from three Youth Internet Safety Surveys (2000, 2005, 2010).*Psychology of Violence*, *3*(1), 53.

Kaplan, G. and Mikes, A. (2012) "Managing risks: a new framework", *Harvard Business Review*, Vol. 90, No. 6, 48–50.

Kraemer, S, Carayon, P. and Clem, J. (2009) "Human and organizational factors in computer and information security: pathways to vulnerabilities", *Computers and Security*, Vol. 28, 509–520.

Livingstone, S, and Helsper, E. (2007). "Gradations in digital inclusion: Children, young people and the digital divide." *New media & society* 9.4: 671–696.

Moore, A. (2007) "They've never taken a swim and thought about Jaws", *College and University,* Vol. 82, No. 4, 41–48.

Humphreys, E. (2008) "Information security management standards: compliance, governance and risk management", *Information Security Technical Report*, Vol. 13, 247–255.

Kankanhalli, A., Teo, H., Tan, B., & Wei, K. (2003) "An integrative study of information systems security effectiveness" *International Journal of Information Management*, Vol. 23, No. 2, 139–154.

Prensky, M. (2001a) "Digital Natives, Digital Immigrants", *On the Horizon: MCB University Press*, Vol. 9, No. 5, 1–6

Prensky, M. (2001b) "Digital Natives, Digital Immigrants Part II: do they really think differently?" *On the Horizon: MCB University Press*, Vol. 9, No. 6, 1–9.

Prensky, M. (2009) H. Sapiens Digital: from Digital Immigrants and Digital Natives to digital wisdom [online] Available at: http://www.uh.cu/static/documents/TD/H.%20Sapiens%20Digital.pdf

Ruighaver, A., Maynard, S. and Chang, S. (2007) "Organisational security culture: extending the end-user perspective". *Computers & Security,* Vol. 26, No 1, 56–62.

Simons, R. (1999) "How risky is your company?" *Harvard Business Review* Vol. 77 No. 5, 85–94.

Siponen, M. and Willison, R. (2009) "Information security management standards: problems and solutions", *Information & Management*, Vol. 46, 267–270.

Techdirt (2014). "UK Web Filtering Blocks Access To Website Of Europe's Largest And Oldest Hacking Community". https://www.techdirt.com/articles/20141208/06160229348/uk-web-filtering-blocks-access-to-website-europes-largest-oldest-hacking-community.shtml. Accessed May 2015.

UK Government (2015). "Statutory guidance: National curriculum in England: computing programmes of study" https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study. Accessed May 2015.

Weick, K. and Sutcliffe, K. (2007). *Managing the unexpected: Resilient performance in an age of uncertainty*, John Wiley and Sons, San Francisco.

Zemke, R., Raines, C. & Filipczal, B. (2000). *Generations at work: Managing the clash of Veterans, Boomers, Xers, and Nexters in your workplace.* Chicago: Amacom.

Endnotes

1. http://www.bbc.co.uk/news/uk-31920906. (Accessed May 2015)
2. http://www.fasken.com/files/upload/Andrews_v_Deputy_Head.pdf. (Accessed May 2015)
3. http://www.computerworld.com/article/2600774/cloud-computing-hacked-naked-selfies-stick-around-celebrity-icloud-sex-download-fears.html. Accessed May 2015.
4. https://www.commonsensemedia.org/. Accessed May 2015.
5. http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/. Accessed May 2015.
6. http://uk.practicallaw.com/6-513-3252. Accessed May 2015.
7. http://uk.practicallaw.com/6-513-3271. Accessed May 2015.
8. http://www.employmentcasesupdate.co.uk/site.aspx?i=ed13900. Accessed May 2015.
9. http://www.xperthr.co.uk/editors-choice/facebook-entry-and-youtube-video-led-to-amateur-models-dismissal/104503/. Accessed May 2015.
10. http://www.telegraph.co.uk/technology/facebook/9155368/Companies-asking-for-Facebook-passwords-for-future-employees.html. Accessed May 2015.
11. http://www.usatoday.com/story/money/business/2014/01/10/facebook-passwords-employers/4327739/. Accessed May 2015.
12. http://www.independent.co.uk/news/uk/politics/brooks-newmark-on-sexting-scandal-i-was-a-complete-fool-9760485.html. Accessed May 2015.
13. http://www.legalcheek.com/2014/10/wannabe-solicitors-career-hopes-in-tatters-after-slapping-woman-in-face-with-penis/. Accessed May 2015.
14. http://www.dailymail.co.uk/news/article-2803524/Student-jailed-slapping-sleeping-woman-face-penis-friend-filmed-phone.html. Accessed May 2015.
15. See: http://www.theguardian.com/money/2007/feb/15/business.accounts. Accessed May 2015.
16. Another good source of practical information comes from BS 65000 Guidance for Organisational Resilience, see http://shop.bsigroup.com/ProductDetail/?pid=000000000030258792 for further information. Accessed May 2015.
17. For a good introduction to the use and management of big data within organisations see: http://erm.ncsu.edu/library/article/big-data-risk-management. Accessed May 2015.